

Modelling Unexpected Failures with a Hierarchical Bayesian Model

Zhiguo Zeng

Chair on System Science and the Energy Challenge,
Fondation Électricité de France (EDF),
CentraleSupélec, Université Paris-Saclay,
3 Rue Joliot Curie, 91190 Gif-sur-Yvette, France
e-mail: zhiguo.zeng@centralesupelec.fr

Enrico Zio

Chair on System Science and the Energy Challenge,
Fondation Électricité de France (EDF),
CentraleSupélec, Université Paris-Saclay,
3 Rue Joliot Curie, 91190 Gif-sur-Yvette, France;
Energy Department
Politecnico di Milano, 20133, Milano, Italy
e-mail: enrico.zio@centralesupelec.fr,
enrico.zio@polimi.it

Abstract—Systems, especially those in the design and development phase, frequently suffer from unexpected failures, which are caused by insufficient knowledge of the system failure processes. In this paper, we develop a hierarchical Bayesian reliability model that account for unexpected failures. For this, the sample space of all failures is broken down into subspaces of expected failures and unexpected failures. The overall reliability is, then, derived based on the total probability theorem. A Bayesian network model is developed to explicitly compute the probability of unexpected failures. A single board computer reliability analysis is considered and the results show that neglecting unexpected failures overestimates the reliability.

Keywords—reliability; epistemic uncertainty; model uncertainty; parametric uncertainty; unknown unknowns; black swan; Bayesian network

ACRONYMS

BN	Bayesian Network.
CPT	Condition Probability Table.
DAG	Directed Acyclic Graph.
SBC	Single Board Computer.

NOTATIONS

P_E	Probability that failures are caused by expected processes.
$R_E(t)$	Reliability model considering only expected failures.
$R_U(t)$	Reliability model considering only unexpected failures.
S	The space that contains all possible failure events.
S_E	The subspace of expected failures.
S_U	The subspace of unexpected failures.
λ_U	Rate of arrival of unexpected failures.
n_U	Number of observed unexpected failures.

I. INTRODUCTION

Reliability models, such as reliability block diagram, fault tree, physics-of-failure models, *etc.*, have been widely used in practice [1]. An implicit assumption is that, all possible

failure processes are considered in the reliability model. In practice, however, new failure modes and mechanisms manifest themselves, especially in systems at the early design and development phases. For example, metal fatigue was first known to engineers only after the continuous explosions of the airplane Comet in the 1950s and, thus, not considered in the reliability analyses [2].

Unexpected accident scenarios have been discussed extensively in the risk analysis community (*e.g.*, see Aven *et al.* [3, 4]). Kaplan *et al.* proposed a Bayesian framework to consider unexpected scenarios, in which a scenario called “others” is added to account for them [5]. The total risk is calculated based on total probability theorem and can be updated using Bayesian methods, when new observation data become available [5]. Kazemi and Mosleh applied a similar method in [5] to investigate the impact of surprising events on credal risks [6]. Aven *et al.* proposed that the likelihood of having unexpected or surprising events are inversely dependent on the knowledge of the analysts, and developed an assumption-deviation method for risk assessment considering surprising events [3].

Existing methods mainly consider unexpected scenarios in risk assessment. However, few researches have been conducted to consider the impact of unexpected failures on reliability. Furthermore, in the existing methods, the probability of unexpected events is assessed by expert judgement. In this paper, we extend the model in [5] and develop a hierarchical Bayesian model for reliability assessment accounting for unexpected failures. A Bayesian Network (BN) model is developed to evaluate the probability of unexpected failures in an explicit way.

The rest of this paper is organized as follows. A hierarchical Bayesian reliability model is developed in Sect. II to consider the influence of unexpected failures. In Sect. III, we present the developed BN for assessing the probability of unexpected events. A reliability analysis of a Single Board Computer (SBC) is conducted in Sect. IV. Finally, this paper is concluded in Sect. V, with a discussion on future works.

II. A HIERARCHICAL RELIABILITY MODEL CONSIDERING UNEXPECTED FAILURES

To account for the effect of unexpected failures, we assume:

- 1) The space that contains all possible failure events is denoted by S and divided into the subspace of expected failures, denoted by S_E , and the subspace of unexpected failures, denoted by S_U :

$$S = S_E \cup S_U. \quad (1)$$

- 2) S_E and S_U are mutually exclusive:

$$S_E \cap S_U = \emptyset. \quad (2)$$

From Assumptions 1 and 2, the can be calculated using the total probability theorem:

$$\begin{aligned} R(t) &= Pr(T > t) \\ &= R_E(t) \cdot P_E + R_U(t) \cdot (1 - P_E), \end{aligned} \quad (3)$$

where P_E is the probability of expected failures, and $R_E(t)$ and $R_U(t)$ represent the reliability with respect to expected and unexpected failures, respectively.

To quantify (3) in practice, models for $R_E(t)$, $R_U(t)$ and P_E need to be developed. Conceptually, we assume that, the reliability with respect to expected failures is modeled as:

$$R_E(t) = g(t | \theta_p) + \epsilon, \quad (4)$$

where $g(\cdot)$ is a probabilistic reliability model, whose parameters θ_p is subject to parametric uncertainty, represented by a probabilistic distribution f_{θ_p} , i.e., $\theta_p \sim f_{\theta_p}$; $\epsilon \sim \text{Normal}(0, \sigma_m^2)$ describes structural uncertainty of the reliability model [2, 7].

Bayesian models are developed for P_E and $R_U(t)$, so that prior expert knowledge and observation data (if available) can be combined to obtain an integrated reliability estimations. For P_E , it is assumed that its prior distribution is a Beta distribution, for calculation purposes:

$$P_E \sim \text{Beta}(K\theta, K(1 - \theta)), \quad (5)$$

where K is the prior sample size and a larger value of K indicates that we have more trust on the prior distribution; θ is the prior mean, which is an a priori estimation of P_E based on the prior knowledge. Beta distribution is chosen because it is the conjugate distribution of the binomial likelihood function, i.e., if we test n samples and observe n_U unexpected failures, the posterior distribution of P_E can be updated by:

$$P_E \sim \text{Beta}(K\theta + n_U, K(1 - \theta) + (n - n_U)). \quad (6)$$

For $R_U(t)$, it is assumed that occurrences of unexpected failures follow a homogeneous Poisson process with a rate λ_U and, therefore, $R_U(t)$ is calculated by:

$$R_U(t) = e^{-\lambda_U t}. \quad (7)$$

The parameter λ_U is assumed to follow a Gamma prior distribution, for calculation purposes:

$$\lambda_U \sim \text{Gamma}(\alpha, \beta). \quad (8)$$

The physical meanings of α and β are that our prior knowledge on λ_U is equivalent to a “pseudo test”, in which we observe α unexpected failures in a total test time β . Therefore, the prior mean for λ_U is α/β . The reason for choosing a Gamma prior (8) is that, it is the conjugate prior for the exponential likelihood (7), i.e., if we observe n_U unexpected failures with times-to-failure t_1, t_2, \dots, t_{n_U} , then λ_U can be updated by

$$\lambda_U \sim \text{Gamma}\left(\alpha + n_U, \beta + \sum_{i=1}^{n_U} t_i\right). \quad (9)$$

III. QUANTIFYING UNEXPECTED FAILURES USING BNs

To apply the model in Sect. II in practice, the prior distributions for P_E and λ_U need to be determined based on our prior knowledge. Traditionally, this is done by directly asking experts to estimate them. This procedure, while operational in practice, remains opaque and subjective. In this paper, we develop a BN model to explicit the prior knowledge on P_E and λ_U , so that their prior estimation can be done in a more transparent way.

A BN is a probabilistic Directed Acyclic Graph (DAG) that describes causal dependencies among the nodes in the graph. The dependencies are described by the directed links between the nodes. Each node is associated with a Condition Probability Table (CPT) that gives the condition probability of observing its values given its parent nodes. Probabilistic reasoning can, then, be conducted applying the Bayesian theorem.

The structure of the BN for assessing the prior distribution of P_E is given in Figure 1. We consider three levels of P_E magnitude, as shown in Table I. For all levels, the prior distribution of P_E has prior sample size $K = 10$ but different prior means, as shown in Table I.

TABLE I. THREE LEVELS OF P_E MAGNITUDE

Level of P_E	K	θ
Low (L)	10	0.1
Medium (M)	10	0.5
High (H)	10	0.9

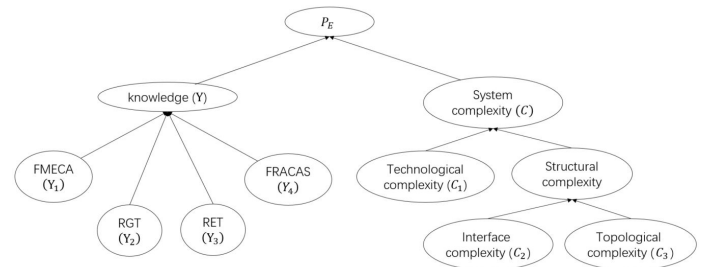


Figure 1. BN model for θ and λ_U

As P_E relates to insufficient knowledge on the system failure processes and consequent incompleteness of their modelling and analysis, we consider two major factors: knowledge, denoted by Y and system complexity, denoted by C .

Knowledge Y quantifies how much we know about the system and its failure processes. Such knowledge is gained through engineering analyses. The more we know about the system through these analyses, the less likely unexpected failures are. On the other hand, system complexity inherently hides unexpected failures: the more complex the system is, the more likely it is that the analysis misses unexpected failures.

Three discrete levels (low, medium and high) are defined for Y and C . Probabilistic dependencies among Y , C and P_E are described by a CPT, denoted by $p(P_E | Y, C)$, which is constructed based on expert knowledge. The obtained knowledge Y is further broken down into the knowledge Y_1, Y_2, Y_3, Y_4 derived from engineering analyses of the system. These engineering analyses include, for example, Failure Modes, Effects and Criticality Analysis (FMECA), Failure Report, Analysis, and Corrective Action System (FRACAS), Reliability Growth Test (RGT), Reliability Enhancement Test (RET) [2]. Their contributions to knowledge achievement are tabulated in Table II. It is assumed that each of the knowledge contributors Y_1 - Y_4 of the engineering analyses takes three discrete values (problematic, satisfactory, ideal) and they are evaluated based on predefined scoring criteria in [2]. As $p(P_E | Y, C)$, a CPT $p(Y | Y_1, Y_2, Y_3, Y_4)$ is defined to describe the dependencies of Y on the knowledge contributors $Y_i, i = 1, 2, 3, 4$, often determined by expert knowledge.

On the other hand, C is also decomposed into topological (C_1), interface (C_2) and topological complexity (C_3), which can be evaluated following the guidelines provided in [8]. The definitions and evaluation guidelines for C_1 - C_3 are given below.

- Technology complexity measures how mature the technologies used in the system design are. In this paper, we use

$$C_1 = \sum_{i=1}^n 5 \left(\frac{T_{\max} - T_i}{T_{\max} - T_{\min}} \right) \quad (10)$$

where $C_1 \in [0, 5]$ and a higher value of C_1 indicates higher technology complexity; T_i is the technology readiness level of the i th component and is evaluated using the 1-9 scoring system of NASA [9]; T_{\max} and T_{\min} are the maximum and minimum possible values for technology complexities, respectively.

- Interface complexity results from the interfaces among the components in the system. It is measured based on the connectivity matrix A of the components [8]:

$$C_2 = \frac{1}{n} \sum_{i=1}^n \sum_{j=1}^n A_{ij} \quad (11)$$

where $C_2 \in [0, n]$ and a high value of C_2 indicates high interface complexity; A_{ij} is the ij th element in the connectivity matrix A ; $A_{ij} = 1$ when component i is connected to j and $A_{ij} = 0$ otherwise.

- Topological complexity depends on the structure of the connectivity matrix A [8]:

$$C_3 = \frac{E(A)}{n} \quad (12)$$

where $E(A) = \sum_{i=1}^n \sigma_i$ and σ_i is the i th singular value of A . It can be verified that $C_3 \in [0, \infty)$ and a large value of C_3 indicates high topological complexity.

The system complexity C , is, then, calculated by [8]:

$$C = C_1 + C_2 C_3. \quad (13)$$

In practice, the evaluation starts from the source nodes Y_i and C_i . For Y_i s, three discrete levels, *i.e.*, problematic, satisfactory and ideal are defined, and an evaluation is carried out following the scoring criteria defined in [9]. For C_i s, the evaluation is carried out first, and then, the C_i s are aggregated to calculate the system complexity C using (13).

Based on the BN in Figure 1, the posterior distribution of θ can be calculated as:

$$p(\theta) = p(\theta | y, C) \cdot \sum_y p(y | y_1, y_2, y_3, y_4) \cdot p(y_1) \cdot p(y_2) \cdot p(y_3) \cdot p(y_4) \cdot p(C) \quad (14)$$

IV. CASE STUDY

In this section, we apply the developed model to the reliability analysis of a SBC (Figure 2 [10]). Traditional reliability evaluation of the SBC is often conducted using the parts-count method in handbooks like Telcordia SR-332 [11], where the system reliability of the SBC is assumed to follow an exponential distribution and its failure rate λ_{SBC} is calculated by

$$\lambda_{SBC} = \pi_E \sum_{i=1}^n N_i \lambda_i, \quad (15)$$

where π_E is an adjustment factor to reflect the difference in operating environment, N_i is the number of the i th component in the SBC, and λ_i is the equivalent failure rate for the i th component, which is estimated from historical failure data of similar products. Using (15) is equivalent to assuming that the system is configured in a series structure and each component has exponential lifetime distribution.

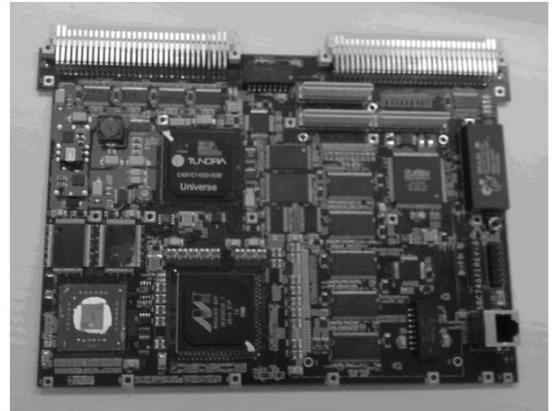


Figure 2. A SBC [10]

The failure rate of each type of components in the SBC is given in Table III. Based on the data in Table III, the reliability

TABLE II. KNOWLEDGE CONTRIBUTIONS OF ENGINEERING ANALYSES

Activities	Knowledge contributions
FMECA	FMECA helps designers to identify potential failure modes and understand their effects.
FRACAS	By implementing FRACAS, knowledge on potential failure modes and mechanisms is gained based on previously occurred failures and corrective actions.
RGT	In RGT, cycles of Test Analysis and Fix (TAAF) are repeated until the product reaches its reliability requirements. By dosing so, designers' knowledge on the failure modes and mechanisms is gained.
RET	RET stimulates potential failures, by highly accelerated stresses, which can generate failures that are hard to be identified by conventional tests.

TABLE III. FAILURE RATES FOR THE SBC COMPONENTS[10]

Component	Failure rate ($\times 10^{-9} \text{ h}^{-1}$)	Number of components
IC	384.8	51
Crystal oscillator	56	4
Inductance	6.56	6
Connector	32.76	9
Capacitor	40.5972	631
Resistance	648.9108	545
Others	16.16	20

of the SBC is

$$R_{SBC}(t) = e^{-1.186 \times 10^{-6} t}. \quad (16)$$

Now, we apply the modelling framework introduced in Section III to account for unexpected failures. For simplicity, but without loss of generality, we do not consider structural uncertainty and parametric uncertainty in (4). Then, R_E is determined by (16). We assume that the prior distribution of λ_{UF} is a *Gamma*(α, β) with

$$\alpha = 10, \beta = \frac{\alpha}{10\lambda_E},$$

which indicates a prior sample size of 10 and a prior mean of $\alpha/\beta = 10\lambda_E$, where λ_E is the failure rate for expected failures, since unexpected failures often occur early in the life cycle and lead to “infant mortality”.

To assess P_E , $Y_i, i = 1, 2, 3, 4$ are evaluated based on the criteria in [2], which leads to

$$Y_1 = 0, Y_2 = 1, Y_3 = 1, Y_4 = 3.$$

To consider complexity, the system architecture of the SBC is given in Figure 3. Based on Figure 3, C_1, C_2 and C_3 can be calculated using (10),(11) and (12), respectively:

$$C_1 = 1.25, C_2 = 2.6, C_3 = 0.8654.$$

Then, from (13), we have $C = 3.5$, which indicates that the SBC has low complexity.

Applying the probabilistic reasoning procedure in (14), we obtain the prior distribution for the P_E , where $P_E \sim \text{Beta}(K, \theta)$ and the values for K and θ are given in Table IV.

The reliability of the SBC, is, then, predicted using (3). The results are given in Figure 4, where the uncertainty bounds are determined by considering the prior distributions in (3). It can be seen that considering unexpected failures leads to

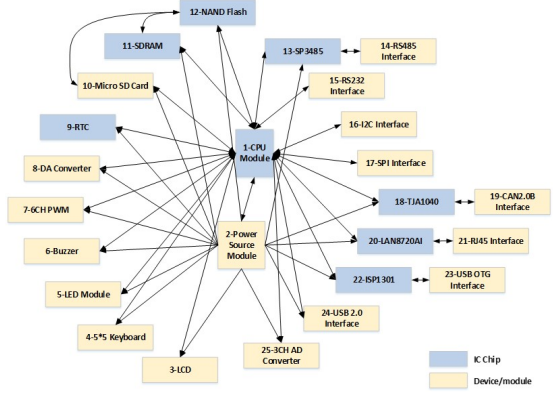


Figure 3. Architecture of the SBC

TABLE IV. PRIOR PROBABILITIES OF P_E LEVELS

Levels of P_E	K	θ	Probability
Low (L)	10	0.1	0.46
Medium (M)	10	0.5	0.52
High (H)	10	0.9	0.02

lower reliability estimations and larger uncertainty. Hence, neglecting unexpected failures might overestimate reliability.

Sensitivity analyses are finally conducted to investigate the influence of knowledge and system complexity on reliability. From the comparison in Figure 5, it can be seen that when the effectiveness of the engineering analyses increases, the knowledge on the system enhances, and, therefore, the possibility of having unexpected failures decrease. On the other hand,

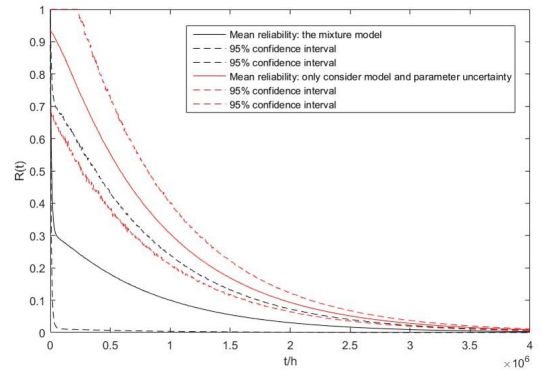


Figure 4. Reliability considering unexpected failures

from Figure 6, it can be seen that when system complexity increases, the possibility of having unexpected failures also increases, and, therefore, the estimated reliability decreases.

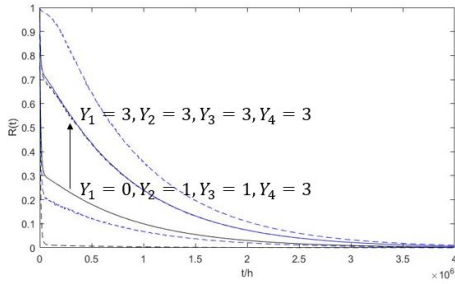


Figure 5. Sensitivities on Y_1 - Y_4

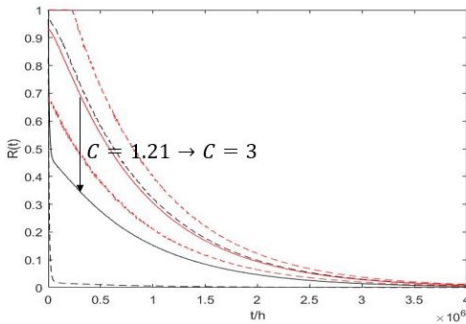


Figure 6. Sensitivities on C

V. CONCLUSIONS

In this paper, we have proposed a hierarchical Bayesian model to estimate reliability accounting for unexpected failures. BNs are used to explicitly quantify the model. A case study on a SBC is used to demonstrate the application of the model for reliability analysis. How to use failure data (from both expected and unexpected failures) collected during operation to update the estimated reliability is a future research step.

REFERENCES

- [1] E. Zio, "Reliability engineering: Old problems and new challenges," *Reliability Engineering & System Safety*, vol. 94, no. 2, pp. 125–141, 2009.
- [2] Z. Zeng, R. Kang, M. Wen, and E. Zio, "A model-based reliability metric considering aleatory and epistemic uncertainty," *IEEE Access*, vol. 5, pp. 15505–15515, 2017.
- [3] T. Aven, "Practical implications of the new risk perspectives," *Reliability Engineering & System Safety*, vol. 115, pp. 136–145, 2013.
- [4] T. Aven and R. Steen, "The concept of ignorance in a risk assessment and risk management context," *Reliability Engineering & System Safety*, vol. 95, no. 11, pp. 1117–1122, 2010.
- [5] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," *Risk analysis*, vol. 1, no. 1, pp. 11–27, 1981.
- [6] R. Kazemi and A. Mosleh, "Improving default risk prediction using bayesian model uncertainty techniques," *Risk Analysis*, vol. 32, no. 11, pp. 1888–1900, 2012.
- [7] Z. Zeng, R. Kang, M. Wen, and E. Zio, "Uncertainty theory as a basis for belief reliability," *Information Sciences (Available Online)*, 2017.
- [8] K. Sinha *et al.*, *Structural complexity and its implications for design of cyber-physical systems*. PhD thesis, Massachusetts Institute of Technology, 2014.
- [9] D. Guide, "Technology readiness assessment (tra)," *Technology Maturation Plan (TMP) Process Guide*, 2008.
- [10] R. Cao, Y. Chen, and R. Kang, "Electronic product reliability prediction methods and case studies based on bellcore standards [j]," *Electronics Quality*, vol. 6, p. 026, 2010.
- [11] T. Technologies, "Special report sr- 332: Reliability prediction procedure for electronic equipment," *Piscataway, Telcor- dia GustQmer ServiGe*, vol. 1, no. 6, 2001.